Navigating Compliance: A Comprehensive Approach for Federal Civilian Agencies

Ensuring Mission Success Through Mandate-Aligned Cybersecurity

Federal civilian agencies face unique challenges when it comes to ensuring the security of their data, systems, and infrastructure. With an ever-evolving threat landscape, rapid technological advancements, and adversarial risks, Maximus's proven approach offers essential, comprehensive support for federal compliance mandates to drive missions forward.

A comprehensive compliance approach: agile, flexible, intelligent

While ensuring alignment with specific mandates is essential, cybersecurity compliance today is not simply a matter of checking the boxes of static regulatory requirements. As mandates are added or evolve over time, a risk-based approach can help define and prioritize security controls. An agile, flexible, intelligent cybersecurity framework helps prepare agencies to respond to changing technological and threat environments, as well as new regulations implemented to address them.

Maximus provides this flexibility, helping to ensure government customers are prepared to meet requirements in place today and respond to others in the future. Our comprehensive compliance is grounded in holistic security integrated into every layer of the organization's IT infrastructure.

Maximus compliance pillars: Your mission, uninterrupted

Automated Authority to Operate (ATO). Federal agencies can ensure mission continuity with an automated ATO approach that provides broad, efficient validation of systems and software for continuous operation. Maximus leverages AI-powered tools for context-based prioritization of security controls and automated collection of documentation, logs, and compliance artifacts. Our approach helps government customers improve ATO efficiency by:

Together, a risk-based approach along with ZTA shifts security from static and reactive to dynamic, continuous, and intelligent–building lasting organizational resilience.

- Minimizing manual search and collection efforts and shortening compliance process timelines
- Leveraging dynamic and responsive monitoring that alerts system owners to issues before they become ATO risks
- Reducing the need for manual intervention in the ATO process

Governance and Policy. Effective governance and policy is about understanding security context, being agile and adaptable, and continuously refining approaches as compliance needs and security environments shift. Maximus provides trusted guidance to federal customers for operationalizing compliance policies and governance practices throughout the enterprise. We work with government partners to:

- Craft robust, agency-wide compliance policy and governance procedures in collaboration with chief information officers and other senior cybersecurity leadership
- Work alongside government teams to execute policies across all operations
- Refine and modify policies as needed in alignment with real-world implementation experience
- Evolve policies away from checklist-based exercises to dynamic, risk-based, data-driven models
- Identify future opportunities and challenges for compliance policy and governance, including balancing human oversight with adoption of AI-powered tools
- Participate in collaborative, cross-agency policy development, such as refinements to standards such as the Joint Implementation Technical Guide

Remediation Management. Effective remediation management is central to ensuring cybersecurity compliance with key mandates. Robust plans enable proactive identification and classification of vulnerabilities and risks, clear incident response procedures, and strategies for continuous monitoring and improvement to decrease the likelihood of encountering the same issue in the future. Maximus empowers federal agencies with industry-leading technologies to:

Compliance Pillars

Enable a Risk-based Approach

- Prioritize vulnerabilities through nuanced analysis of end users, systems, applications, and other assets

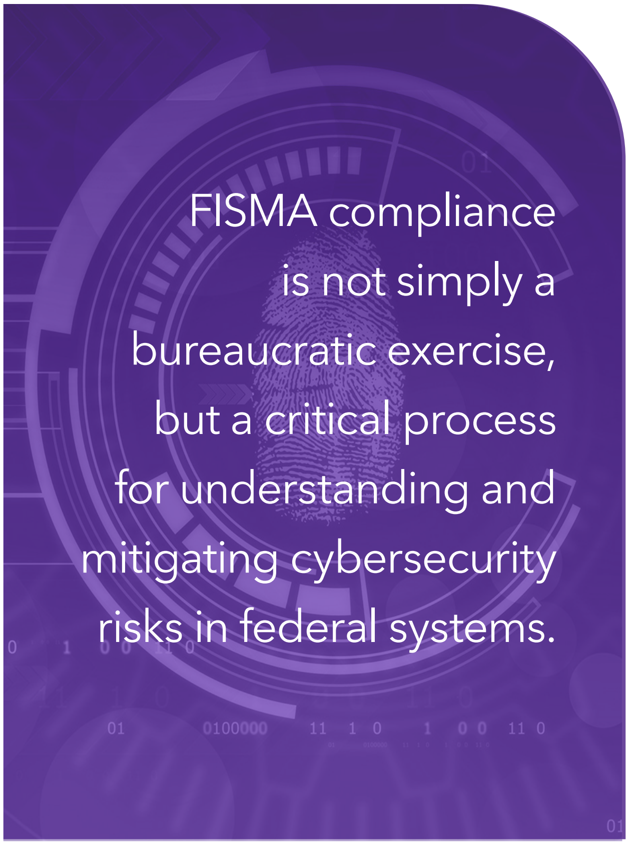
Leverage User Behavior Analytics

- Leverage user behavior analytics and threat intelligence to understand user-level risks and behaviors and implement just-in-time and just-enough access principles to minimize vulnerabilities

Implement AI-powered Tools

- Implement AI-powered tools to aggregate cybersecurity incident data and automate (or even suggest) remediation steps

These compliance pillars are grounded within an end-to-end risk-based cybersecurity approach executed through Zero Trust Architecture (ZTA) principles, helping achieve focused security operations. ZTA provides the tools to assess



FISMA compliance is not simply a bureaucratic exercise, but a critical process for understanding and mitigating cybersecurity risks in federal systems.

risk and apply precise protections to secure the organization's most critical assets. Together, a risk-based approach along with ZTA shifts security from static and reactive to dynamic, continuous, and intelligent—building lasting organizational resilience.

Compliance with key cybersecurity mandates

Integrating industry-leading risk management frameworks and advanced cyber technologies helps ensure your digital landscape is protected while meeting the highest levels of compliance. Maximus works in partnership with federal civilian agencies to ensure cybersecurity compliance with all major mandates, including:

Federal Information Security Management Act (FISMA)

As a trusted government contractor, Maximus operates within the framework of FISMA compliance, adhering to the Act's mandates for cybersecurity measures for federal agencies and their contractors.

Our cybersecurity experts have a deep understanding of the Act's requirements from both government and corporate perspectives, as demonstrated by our own FISMA authorization boundary and FedRAMP authorization. We work with government customers to ensure annual FISMA compliance, including:

- **Ensuring continuous monitoring of all IT systems,** enabling agencies to respond rapidly to security incidents or data breaches
- **Establishing an inventory of IT systems,** ensuring that our team and our government customers have a full picture of their security landscape and potential attack surface
- **Performing system risk security categorization** of IT assets as defined by the National Institute of Standards and Technology (NIST) to align asset security levels with their risk levels
- **Establishing a system security plan** including security controls and their implementation, enabling security transparency and accountability
- **Implementing and documenting baseline security controls,** demonstrating that government assets meet minimum relevant security requirements as defined by NIST
- **Conducting regular risk assessments** to ensure validation of current security controls and enabling security teams to determine if additional measures are needed
- **Performing annual security reviews** to ensure current FISMA certification and accreditation

While these activities are foundational, Maximus works with government customers to understand and execute FISMA compliance not simply as a bureaucratic exercise, but as a critical process for understanding and mitigating cybersecurity risks in federal systems. This means implementing holistic, risk-based analyses across the entire IT infrastructure to continuously evaluate security measures and threat levels and allocate resources efficiently based on an evolving risk landscape.

Executive Orders Aimed at Improving Federal Cybersecurity

Maximus works diligently with our federal civilian agency partners to implement security approaches in alignment with executive orders aimed at improving cybersecurity across the federal enterprise. Notably, Executive Order 14028, "Improving the Nation's Cybersecurity" provided a significant step toward more intelligent, context-aware cybersecurity approaches for federal agencies. Largely in effect under the current administration, the order advocates for federal agencies to make progress toward cyber modernization by rethinking how they develop and secure systems and promote a more dynamic, risk-aware security model.

The Maximus cybersecurity approach for federal customers is aligned with the modernization priorities of the order, including:

- **Adopting ZTA** across all cybersecurity tools and technologies, along with roadmaps and resources to achieve an optimal Zero Trust environment
- **Prioritizing supply chain risk management,** helping agencies mitigate the security risks introduced by IT assets from outside vendors
- **Migrating to secure cloud services** with robust, built-in security features, automated updates, AI-powered enhanced threat detection, and continuous monitoring to potentially reduce attack surface and minimize the risks associated with on-premises infrastructure
- **Implementing enhanced security measures**, including multi-factor authentication and encryption to protect sensitive data, particularly personally identifiable information (PII) within cloud environments
- **Ensuring security incident response**, enabling agencies to rapidly address any malicious cyber activity or threat, recover quickly, and implement measures to mitigate lost data or compromised systems

> Maximus led the first successful migration to cloud infrastructure for a federal regulatory agency, creating a cloud-ready High Value Asset platform with FISMA authorization to ensure continuous compliance with federal security requirements.

NIST Risk Management Framework. The NIST Risk Management Framework (RMF) provides a process that integrates security, privacy, and cyber supply chain risk management activities throughout IT development life cycles. This risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.

The RMF provides instrumental support for the implementation of risk management programs to meet the requirements of FISMA. Maximus's comprehensive compliance approach ensures our federal agency customers align with the RMF's seven-step process that guides organizations to:

- **Prepare** for security management and privacy risks
- **Categorize** systems and information
- **Select** security controls
- **Implement** and document controls
- **Assess** security performance against expected outcomes
- **Authorize** systems for operation based on risk-informed decisions
- **Monitor** security implementations and new potential system threats

Demonstrated impact

Maximus has helped federal agency partners advance cybersecurity and compliance goals as part of overall digital modernization strategies. Key examples of customer success include:

Scaling cyber and cloud modernization for cost efficiency

Maximus supports a key laboratory within the Department of Energy to help drive innovation and deliver solutions for a clean and secure energy future. The lab's digital transformation journey has accelerated key initiatives and projects such as:

- Cybersecurity modernization, including collaboration on the transition to the NIST 800-53 Risk Management Framework (RMF) and development of advanced cyber policies and procedures
- Cloud modernization, including assistance with workflow design, applications refactoring, and implementation of the ongoing project to transition services and systems to Microsoft® Azure cloud
- Enhancing scalability, implementing key aspects of enhanced cyber security policies, and improving the lab's capability for disaster recovery while cutting operational costs

Creating cloud-compliant infrastructure

Maximus led the first successful migration to cloud infrastructure for a federal regulatory agency, creating a cloud-ready High Value Asset (HVA) platform with FISMA authorization to ensure continuous compliance with federal security requirements. Additional cybersecurity achievements included:

- Implementing and maintaining RMF compliance across the agency's enterprise-wide system, which processes approximately 3,500 filings daily
- Closing 30 long-standing milestones in the contract's first year, significantly improving system security posture
- Establishing and maintaining a FedRAMP-authorized environment with the agency website hosted in AWS GovCloud

Providing end-to-end cyber operations and maintenance. Maximus has delivered Satellite Mission Operations and Maintenance Support (SMOMS) for a federal environmental agency with cybersecurity achievements including:

- Implementation of integrated IT security standards throughout the system development lifecycle to improve end-to-end security posture
- Enablement of processes to accurately document performance improvements and security efficiencies to support compliance
- Establishment of a shared services environment, improving both security posture and operational efficiencies

Why Maximus

Operational Expertise

We leverage deep experience managing large-scale operations and data architectures to identify new vulnerabilities, secure against known threats, and ensure government mission success and compliance with current requirements.

Agillity & Innovation

Appraised at CMMI Level 5 – the highest level – for both services and development, we quickly adapt to changing requirements for continuous agility and innovation.

Secure Infrastructures

With FedRAMP Moderate Authorization for cloud environments, we provide a portfolio of managed services including infrastructure (IaaS), platforms (PaaS), and software (SaaS) to meet unique government compliance and security requirements. Our FedRAMP-authorized cloud and security operations center (SOC) services support 10+ federal agency programs. We provide hosting solutions on behalf of government customers that can be used for staging grounds, pre-production, or cybersecurity ranges. With control over our FedRAMP Joint Authorization Board (JAB) boundary, our experts have a comprehensive understanding of the factors involved in securing federal systems.

Technical Expertise

With our incubator environment we foster a culture of continuous learning and growth, led by a team of cybersecurity experts boasting 100+ advanced certifications.

Maximus Cybersecurity Experts

Kynan Carver
Managing Director,
Cybersecurity Technology Services

Michael Sieber
Senior Director,
Cybersecurity Technology Services

Michael Geronimo
Director,
Cybersecurity Technology Services

Certifications and Authorizations

FedRAMP

CMMIDEV/5

CMMISVC/5

ISO 20000

ISO 9001

ISO 27001 Certified

ITIL

PMI PMBOK

maximus @maximus_news maximus.com/technology-services/cybersecurity